Amendments to the Claims:

This listing of claims replaces all prior versions and listings of claims in the application:

Listing of Claims:

1-30. (Cancelled).

31. (Currently Amended) A method for controlling ~~cryptographic~~ functions of an application program, the method comprising:

accessing a policy file ~~that reflects a condition of the policy file and~~ that includes an attribute portion configured to store one or more ~~cryptographic~~ policy attributes and a value portion having one or more attribute values, each attribute value corresponding to a ~~cryptographic~~ policy attribute and indicating whether an application program may use ~~the cryptographic policy~~ a function capable of being performed by the application program and represented by the ~~cryptographic~~ policy attribute, and a signature portion including at least one digital certificate;

determining whether the policy file is unaltered based on the signature portion of the policy file;

~~selectively~~ retrieving at least one of the attributes and, for each retrieved attribute, an attribute value corresponding to the attribute ~~encryption information and decryption information~~ from the policy file;

determining whether a function represented by a retrieved attribute is permitted to be accessed by the application program;

~~selectively processing the retrieved encryption information and decryption information from the policy file in accordance with a predetermined capability condition~~; and

~~providing at least one of allowable encryption levels and decryption levels to~~ permitting the application program to access the function conditioned upon a determination that the policy file is unaltered.

32. (Previously Presented) The method of claim 31 wherein the policy file comprises a JAVA archive file.

33. (Previously Presented) The method of claim 31 wherein the policy file comprises multiple component files, at least one of the component files storing some of the attribute portions and attribute values.

34. (Previously Presented) The method of claim 33 wherein at least one of the multiple component files is associated with a signature portion including at least one digital certificate for ensuring that the policy file has not been modified and a signature portion including at least one digital certificate for ensuring that the policy file has not been modified and applying to a particular component file.

35. (Cancelled)

36. (Currently Amended) The method of claim 31 wherein:

the ~~policy file includes a~~ signature portion applies to the attribution portion and the value portion of the policy file;~~including at least one digital certificate for ensuring that the policy file has not been modified~~

determining whether the policy file is unaltered comprises determining whether the attribute portion and the value portion are unaltered based on the signature portion.

37. (Previously Presented) The method of claim 36 wherein the signature portion applies to the policy file.

38. (Currently Amended) The method of claim 31 wherein:

~~each of the cryptographic policy attributes includes an indication of the cryptographic capabilities of the application program, and~~

each of the attribute values is one of a string, an integer number, and a truth expression.

39. (Previously Presented) The method of claim 38 wherein the truth expression is one of a true flag, a false flag, and a conditional flag.

40. (Currently Amended) An apparatus for controlling ~~cryptographic~~ functions of an application program, the apparatus ~~comprising a processor connected to storage and one or more input/output devices, wherein the processor is~~ being configured to:

access a policy file ~~that reflects a condition of the policy file and~~ that includes an attribute portion configured to store one or more ~~cryptographic~~ policy attributes and a value portion having one or more attribute values, each attribute value corresponding to a ~~cryptographic~~ policy attribute and indicating whether an application program may use a function capable of being performed by the application program and ~~the cryptographic policy~~ represented by the ~~cryptographic~~ policy attribute, and a signature portion including at least one digital certificate;

determine whether the policy file is unaltered based on the signature portion of the policy file;

~~selectively~~ retrieve at least one of the attributes and, for each retrieved attribute, an attribute value corresponding to the attribute ~~encryption information and decryption information~~ from the policy file;

determining whether a function represented by a retrieved attribute is permitted to be accessed by the application program;

~~selectively process the retrieved encryption information and decryption information from the policy file in accordance with a predetermined capability condition~~; and

~~provide at least one of allowable encryption levels and decryption levels to~~ permitting the application program to access the function conditioned upon a determination that the policy file is unaltered.

41. (Previously Presented) The apparatus of claim 40 wherein the policy file comprises a JAVA archive file.

42. (Previously Presented) The apparatus of claim 40 wherein the policy file comprises multiple component files, at least one of the component files storing some of the attribute portions and attribute values.

43. (Previously Presented) The apparatus of claim 42 wherein at least one of the multiple component files is associated with a signature portion including at least one digital certificate for ensuring that the policy file has not been modified and the signature portion applying to a particular component file.

44. (Cancelled)

45. (Currently Amended) The apparatus of claim 40 wherein the ~~policy file includes a~~ signature portion applies to the attribute portion and the value portion of the policy file; ~~including at least one digital certificate for ensuring that the policy file has not been modified~~

determining whether the policy file is unaltered comprises determining whether the attribute portion and the value portion are unaltered based on the signature portion.

46. (Previously Presented) The apparatus of claim 45 wherein the signature portion applies to the policy file.

47. (Currently Amended) The apparatus of claim 40 wherein:

~~each of the cryptographic policy attributes includes an indication of the cryptographic capabilities of the application program, and~~

each of the attribute values is one of a string, an integer number, and a truth expression.

48. (Previously Presented) The apparatus of claim 47 wherein the truth expression is one of a true flag, a false flag, and a conditional flag.